BAB 1
USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Fraud menurut Association of Certified Fraud Examiners (ACFE) adalah laporan keuangan yang keliru atau penipuan yang dibuat oleh suatu entitas atau individu dengan mengetahui bahwa hal tersebut dapat dilakukan untuk memperoleh keuntungan yang tidak sah [1]. Salah satu bentuk fraud adalah pencucian uang. Pencucian uang adalah ketika uang yang bersifat ilegal dipindahkan melalui sistem keuangan untuk membuat uang tersebut terlihat sah. Menurut Panel Tingkat Tinggi International Financial Accountability, Transparency and Integrity (Panel FACTI) sekitar $1,6 Triliun atau setara dengan 2,7% dari PDB global dicuci setiap tahun [2].

Perpindahan atau pertukaran uang dapat dilakukan dengan cepat dan mudah. Perpindahan uang dapat mencapai batas negara bahkan di luar wilayah. Adanya kegiatan transaksi juga disebut perpindahan uang. Menurut Undang-Undang No. 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang, transaksi keuangan adalah transaksi di mana uang ditempatkan, diserahkan, ditarik, ditransfer, atau dilakukan kegiatan lainnya yang terkait dengan uang. Dalam konteks ini, tidak dapat dipungkiri bahwa ada pihak-pihak yang tidak bertanggung jawab yang memicu transaksi keuangan yang mencurigakan. Sebagaimana yang telah dijelaskan oleh Rezim Anti Pencucian Uang, lembaga keuangan atau penyedia jasa keuangan memiliki tanggung jawab penting untuk mendeteksi secara dini adanya transaksi keuangan mencurigakan. Deteksi ini dapat dicapai melalui laporan transaksi keuangan mencurigakan yang dikirim kemudian ke lembaga intelijen keuangan terkait. Jika lembaga keuangan mencurigai atau memiliki alasan yang masuk akal untuk mencurigai bahwa dana yang ada berasal dari kegiatan kriminal atau terkait dengan pendanaan teroris, laporan transaksi keuangan yang mencurigakan dapat dimulai dengan praduga.

Oleh karena itu, sangat penting untuk memeriksa setiap transaksi keuangan yang mencurigakan. Hal ini disebabkan fakta bahwa para pelaku pencucian uang biasanya tidak menghabiskan atau menggunakan properti yang mereka peroleh dari tindakan kriminalnya

secara langsung; sebaliknya, mereka akan memasukan properti tersebut ke dalam sistem keuangan melalui tahap penempatan, pelapisan, atau integrasi. Upaya tersebut dilakukan untuk menyembunyikan asal-usul properti sehingga tampak legal. Pelaku tindak pidana tersebut juga dapat dengan aman menggunakan hasil tindak pidananya.

1.2 Analisa Masalah

1.2.1 Aspek Hukum

Dalam penerapannya, identifikasi transaksi keuangan mencurigakan merupakan salah satu kegiatan yang wajib dilakukan oleh lembaga yang berwenang. Hal ini diperlukan untuk mendukung upaya pencegahan atau pemberantasan tindak pidana pencucian uang dan pendanaan terorisme. Akan tetapi, perlu diperhatikan bahwa tidak semua transaksi keuangan mencurigakan merupakan hasil tindak pidana. Bisa saja transaksi tersebut merupakan transaksi legal yang berasal dari penjualan aset pada waktu tertentu. Oleh karena itu, transaksi keuangan mencurigakan perlu dilaporkan sebagai kewajiban langsung dan tidak langsung bagi lembaga penyedia jasa keuangan. Penuntutan terhadap transaksi keuangan mencurigakan akan ditentukan berdasarkan bukti dan fakta yang ada [3].

1.2.2 Aspek Ekonomi

Pelanggaran pencucian uang memiliki dampak negatif pada sektor ekonomi suatu negara. Hal ini termasuk merusak sektor bisnis swasta yang sah, merusak integritas pasar keuangan, menghilangkan kendali kebijakan pemerintah atas perekonomian, dan menciptakan distorsi dan ketidakstabilan ekonomi. Pencucian uang dapat merusak sektor bisnis swasta yang sah karena sering kali menggunakan perusahaan palsu untuk mencampur uang haram dengan uang yang sah, sehingga menyebabkan perusahaan yang sah kalah dalam persaingan. Selain itu, tindak pidana pencucian uang juga dapat merusak integritas pasar keuangan dengan mengancam likuiditas lembaga keuangan yang terlibat. Pencucian uang juga dapat menghilangkan kendali pemerintah atas kebijakan ekonomi, khususnya terkait nilai mata uang dan suku bunga. Akibatnya, dapat terjadi distorsi dan ketidakstabilan ekonomi yang dapat mengganggu pertumbuhan ekonomi suatu negara [4].

1.2.3 Aspek Teknis

Lembaga keuangan perlu mengimplementasikan strategi dan kontrol yang efektif dalam rangka mencegah dan mendeteksi kegiatan penipuan. Hal ini melibatkan penggunaan teknologi dan metode analisis yang canggih, serta pelatihan yang tepat bagi karyawan untuk

meningkatkan kesadaran akan risiko penipuan dan tindakan pencegahan yang diperlukan. Selain itu, kerjasama dengan lembaga keuangan dan otoritas pengawas juga penting untuk memperoleh akses ke data dan informasi yang diperlukan untuk analisis yang efektif [5].

Untuk memastikan penerapan manajemen risiko yang efektif, bank diharapkan memiliki kebijakan manajemen risiko keamanan siber dan mampu mengidentifikasi, melindungi, mendeteksi, merespon, dan mengatasi ancaman risiko siber. Penerapan manajemen risiko keamanan siber harus disesuaikan dengan tujuan, kebijakan bisnis, ukuran dan kompleksitas usaha, teknologi informasi yang digunakan, serta kemampuan bank [6].

1.3 Analisa Solusi yang Ada

Berdasarkan masalah di atas tentunya solusinya adalah agar pihak penyedia jasa keuangan dapat mendeteksi transaksi mencurigakan tersebut adalah dengan menggunakan aplikasi yang mampu mendeteksi transaksi mencurigakan contohnya seperti IDS, Real Time Anti-Fraud Solution, Sas Anti-Money Laundering, dan IBM Safer Payments.

1.3.1 Input Detection System (IDS)

IDS atau Input Detection System adalah perangkat keras (dapat juga dalam bentuk perangkat lunak) yang memiliki kemampuan untuk mendeteksi aktivitas yang mencurigakan dalam sistem atau jaringan. Ada dua pendekatan pendeteksian IDS: berbasis aturan (berbasis tanda tangan) dan berbasis perilaku. Pendeteksian berbasis tanda tangan mencocokkan lalu lintas jaringan dengan aturan yang dibuat oleh administrator dan disimpan dalam *database*. Pendeteksian jenis ini membutuhkan pembaruan pada *database* aturan untuk melakukan pendeteksian IDS. Dibandingkan dengan pendekatan berdasarkan perilaku, pendekatan berdasarkan perilaku mendeteksi serangan dengan membandingkan pola dari kumpulan data yang berbeda menggunakan metode untuk proses klasifikasi. Kelebihan dari IDS sendiri adalah pemantauan yang dilakukan akan berjalan terus-menerus akan tetapi IDS sendiri sangat sulit untuk dikonfigurasi [7].

1.3.2 Real Time Anti-Fraud Solution

Aplikasi Real Time Anti-Fraud Solution akan menganalisa data secara *real-time* dengan cara kerja memberikan peringatan, menginvestigasi apa yang terjadi, lalu mengambil tindakan yang untuk menghentikan transaksi mencurigakan tersebut, dan juga aplikasi ini bisa melakukan monitoring untuk melihat pola data yang mencurigakan. Kelebihan dan

kekurangan dari aplikasi ini dapat menghasilkan akurasi yang sangat tinggi akan tetapi biaya pemeliharaan sistem dari aplikasi ini bisa dibilang tidaklah murah [8].

1.3.3 Sas Anti-Money Laundering System

Sas Anti-Money Laundering System bekerja dengan cara melakukan pengumpulan data, pemrosesan data, menganalisis data, pengawasan dan peringatan, investigasi dan pelaporan. Kelebihan dan kekurangan dari aplikasi ini yaitu pengawasannya dilakukan secara *real-time* akan tetapi biaya implementasi yang dibutuhkan sangatlah mahal [9].

1.3.4 IBM Safer Payments

IBM Safer Payments bekerja dengan cara melakukan pengumpulan data, pemrosesan data, analisis data, dan juga memberikan peringatan dan tindakan yang dilakukan oleh seseorang terkait dengan pendeteksian *fraud* tersebut [10].

Sistem-sistem yang telah dijelaskan tentunya memiliki kelebihan dan kekurangannya masing-masing dalam melakukan pencegahan transaksi mencurigakan. Sistem-sistem tersebut memiliki kelebihan, di antaranya dapat melakukan analisis dan pemrosesan data secara *real-time* akan tetapi untuk mengoperasikan sistem-sistem tersebut juga dibutuhkan pengguna yang terlatih. Tentunya sistem-sistem tersebut juga memiliki keterbatasan, seperti keterbatasan pengguna atau SDM yang melakukan pendeteksian, keterbatasan bahasa pemrograman yang digunakan pada sistem pendeteksi transaksi mencurigakan, metode pendeteksian belum bisa melakukan pendeteksian dengan sangat handal, dan teknologi pendeteksian yang sangat handal namun belum ditemukan hingga saat ini. Inovasi yang dapat dibuat atas solusi yang sudah ada sebelumnya adalah dengan mengombinasikan setiap teknologi yang tersedia agar dapat melakukan proses pendeteksian transaksi mencurigakan dengan membuat sistem prediktif yang akurat.

1.4 Kesimpulan dan Ringkasan CD-1

Fraud merupakan masalah serius yang harus selalu diwaspadai. Deteksi transaksi keuangan yang mencurigakan menjadi tanggung jawab bagi semua pihak, mengingat pentingnya pencegahan tindak pidana ini. Identifikasi yang akurat sangat penting untuk mendukung upaya penegakan hukum mengingat proses penipuan yang dilakukan oleh pelaku melibatkan langkah-langkah yang rumit. Untuk mengatasi tantangan ini, lembaga keuangan harus mengimplementasikan teknologi yang canggih serta melibatkan kerjasama lintas lembaga untuk mendeteksi aktivitas mencurigakan secara efektif.

Berbagai solusi teknologi memiliki kelebihan dalam hal pemrosesan data secara *real-time*, namun juga memiliki keterbatasan dalam hal biaya implementasi, kompleksitas, dan kebutuhan akan pengguna yang terlatih. Melihat kelebihan dan keterbatasan dari teknologi-teknologi tersebut, dapat diciptakan sebuah inovasi yang tepat dalam meningkatkan efektivitas dan efisiensi dalam melakukan deteksi terhadap transaksi yang mencurigakan.